HACKING

ULTIMATE HACKING FOR BEGINNERS, HOW TO HACK

Andrew Mckinnon

Hacking:

Ultimate Hacking for Beginners

How to Hack

Table of Contents

Introduction

If you ever mention to a 3rd person that you can hack in to a system, there will be two different kinds of reactions you will face. One - you will be looked at as if you are some kind of a thief, while the other will make you feel like you are a genius.

In reality, it is partially a truth that you are a genius but chances are you are a thief too. What makes you a genius is the fact that you have the knowledge and technical knowhow of how to hack in to a system. What makes you a thief is what you do once you hack into a system. If you use the data for anti-social means like monetary benefits or compromising the security of the system, you are a thief.

However, you don't have to be a thief if you a hacker. Hacking can be a fun activity as long as it is harmless. If you are hacking in to a system just to quench your curiosity, then this kind of hacking is fine. Rather many companies will be interested in hiring you as an official hacker to safeguard their systems and security.

Yes, as surprising as it sounds, you can actually make a career out of hacking and can be hired in to esteemed government organizations, can freelance as a private hacker or also work with multinationals; the opportunities are limitless. However, try to keep this activity limited to ethical means and do not venture in to the dark side of hacking.

This book will help you understand about the world of hacking, how you can break down passwords, fight anti-virus and get in to a system. We will also look into the various aspects of hacking. I will provide you with detailed instructions for protecting your personal or office computers from this menace of the World Wide Web.

Use this book to enhance your knowledge about ethical hacking and also as a tool to learn to safeguard your system and improve the safety against the bad guys (unethical hackers)

I want to thank you for choosing this book and hope you find it informative and have a good read.

Chapter 1: Hacking - An Overview

Hacking of computer systems and networks is considered as the biggest national threat by the security services and the intelligence agencies of many countries. Hacking was once considered as a harmless prank. But now hacking is no less of a crime than any other. In some countries hacking is considered on the same level as terrorism. It is condemned large by the world governments.

In simple words hacking is breaking into someone's network or system without permission by compromising their security and stealing their information or damaging their entire system in the worst case.

Way back in the 1960's and 70's members of the youth international party made street pranks by tapping telephone lines. This group mainly comprised of youth. At its initial stages it was countercultural. Gradually this developed into hacking. The pliers and telephone lines were replaced by multifunctional screens and mega core processors.

The goofy nature of hacking was slowly replaced. Hacking, which was once started as a prank by the peace loving activists is now being used by terrorist organizations. They use it for many reasons such as gathering information on military movements, fundraising and for spreading their propaganda.

In this chapter you will get a general idea on what hacking really is and later on the classification of hackers.

In general, hacking is the process of ascertaining and subsequent exploitation of various weaknesses and shortfalls in the network of computer systems or a single computer system. This exploitation can be in the form of changing the structural picture of the computer system, altering the configuration, stealing information etc. But sometimes hacking is used for displaying the system flaws and weak spots.

The wide spectrum of hacking is not just found in developed countries. In the last two

decades, with the large development in the area of information technology, it may surprise you that most of the hackers are from developing countries of Southeast Asia and some part of South Asia.

It is extremely difficult for a particular activity to be considered as hacking or not. This is because of the ambiguity in the world of hackers. Due to this inexactness, the term hacker is hard to explain and has always been a subject of a lot of controversies. The term hacker, in some contexts is used as reference to an individual who has command over the networks and computer systems.

A computer security specialist who finds and fixes the loopholes in the system is also considered as a hacker in some contexts. These people are also sometimes called as crackers. We will learn more about the classification of practicing detail in the second part of this chapter.

There can be many reasons behind hacking. Some hackers do it for the simple reason of money making. These hackers steal and retrieve information from a computer and use it for their monetary gains. Some hackers take it as a mere challenge for doing things that are prohibited and retrieving forbidden information.

While some do it just for fun by accessing a network or a computer system and adding a message. Some do it to disrupt a company or an organization's business and create chaos. Some hack to protest against the government or an organization. They do it by sneaking into the network systems of the authorities instead of raising their voice against them.

Classification – Various kinds

Basing on the modus operandi of the hackers and the intention behind their actions, they can be classified into the following types.

White hat hackers

The white hat hacker is also called as ethical hacker. He is someone in the area of information technology, who opposes the abuse of networks and computer systems.

They hack but not with the intention to deceive. They perform a series of tests that check the efficacy of their company's or organization's security systems. These companies are usually computer security software manufacturers. Their main purpose is to carry out penetration tests and vulnerability assessments. These are the people who stand between Black Hat hackers and companies.

Black hat hackers

A black hat hacker is the opposite of the white hat hacker or the Ethical hacker in both methodology and intention. These hackers violate the computer systems or a network with intentions for personal and monetary gains. These are the ones who are commonly perceived as hackers. They are the illegal communities and are stereotypes of computer criminals.

They gain access into a network with intent of modifying, stealing or destroying the data. They modify the program in a way that the user cannot use it. They find a vulnerable area or a weak spot. Using this they gain access to the system. The proprietors, general public and the other days are kept in the blind from such vulnerabilities.

Grey hat hackers

The color grey is a mix of both black and white. Similarly the grey hat hackers are an interesting mix of both white hat and black hat characteristics. The grey hat hackers usually trawl the Internet seeking for faults in the network and then hack into them. Demonstrating the security flaws of a network to their administrators is their main intention. The grey hats hack into their networks and may offer to fix the security flaws after diagnosis for a suitable consideration.

Blue hat hackers

The blue hat hackers are freelancers. The computer security firms hire them for their expertise. They are called by the security companies to check for vulnerabilities in their systems. This was before the new system was introduced.

Elite hackers

The elite hackers are the best of the hacking community. They write programs and are usually the 1st to break into an impenetrable system. The elite hackers avoid destroying the data from the computer systems that they have exploited. Each hacking community has their own elite hackers. There elite status is given to them by their

community. They demote the most proficient of the hackers.

Skiddie

"Skiddie" is the short term form "Script Kiddie". Skiddies are basically amateurs who manage to hack into the system and access them by using the programs given out by elite hackers or other expert level hackers. Though they use the programs, they have no knowledge on the programs they use.

Newbie

The name tells it all. They are the beginners in the hacking world. Newbies have no knowledge or any prior experience with them. They hang around with others in the hacking community with the motto of learning the tips and tools of hacking.

Hacktivism

In this version of hacking, the hackers use their skills to publish a social or a religious message. They do it with the systems or networks they hacked into. This is of two types

1. Right to information
2. Cyber terrorism.

The Right to information group hacks into a system with the intent of gathering information which is confidential from public and private sources and give it to the public domain.

The cyber terrorism has the sole purpose of destroying the system's operation and making it useless.

Intelligence agencies

Intelligence agencies are hackers who work for the safeguarding of the national systems from foreign threats. This actually cannot be considered as hacking as they hack for protecting the state's interests. These agencies usually hire Blue hat hackers. This is a kind of defence strategy.

Organized crime

This can be considered as a group of black hat hackers on other expert level hackers who are working under are particular community with a common goal. They break into the systems of private organizations and government authorities. With the obtained information, they aid the criminal objectives their group has.

Chapter 2: Hacking Tools

Hacking tools are software programs designed to help hackers gain unauthorized access to a computer system.

Vulnerability Scanner

Vulnerability is defined as an unintended software flaw and can be used as an opening used by hackers to sending malicious software like Trojan horses, viruses, worms etc.

A Vulnerability scanner is a very efficient tool used for checking weak spots in a computer system or a network. It is basically a computer program. The sole purpose of the scanner is to access networks, applications and computer systems for weaknesses. This is used by both Black Hat hackers and computer security managers who are usually White hat hackers or blue hat hackers. The black hat hackers use this for checking for weaknesses and gain unauthorized access from those points. In the hands of white hat hackers this is used for the same purpose of checking for weaknesses but they use it for protecting the computer systems.

The data is transmitted through the ports. The vulnerability scanner is used for checking the ports which are open or which have available access to a computer system. This is used for quickly checking the network for computers with known weaknesses. By limiting the ports, the firewall defends the computer, although it is still vulnerable.

Types of vulnerability scanners

Port scanner:

A port scanner is a computer application which is solely designed for searching open ports on a server or a host. The person who intends to use this should have basic knowledge on TCP/IP. The attackers use this for the identification of running services on a server or a host with the intention of compromising it. The administrators on the other hand use this to verify their network's security policies. A port scan is a process which sends requests to a selected range of ports with the agenda of finding an active port. This can only find vulnerability and cannot be used for attacking or protecting. Most of the uses of this scan are just probes and not attacks.

Network vulnerability scanner

The purpose of this scanner is to check for weaknesses on the network with which the

computer systems are connected. The hacker looks for a weakness in a network with this scanner and can break into the system.

Password Cracking

Password cracking is the process of recovering passwords, which are transmitted and stored in the computer system. With this, you can gain access to a computer system by gaining the password of the user. The time required for cracking password depends entirely on the strength of the password used. Most of the methods used usually require the computer system for producing many passwords, which are then checked individually.

There are many methods for cracking passwords. Brute force is one of them. It is a time taking process as it uses all possible combinations of letters and words until it succeeds. Methods like word list substitution, but on checking, dictionary attacks are performed before using brute force. This is done to reduce the number of attempts.

Packet Sniffer

Packet Sniffers are also called as protocol analyzers. They can be used for collecting passwords using packet capture and injection tasks. As we know, the data is sent in the form of packets. So if you can retrieve the packets sent or received, he can have access to the password or any other data which is transmitted. Packet sniffers intercept the network traffic.

Spoofing Attack (Phishing)

Spoofing is nothing but making a fake website or program which looks like the original. User gets fooled thinking that it is the original website or program. The main purpose of spoofing attack is to collect confidential information such as ID and passwords.

There are many types of spoofing. Some of them are

1. Referred spoofing: Some website only allows access from a given set of approved login pages. Here the HTTP request is checked. And only referred headers are allowed. This allows them to gain unauthorized access.

2. Email address spoofing: This type of spoofing is commonly used by spammers to hide the content and mislead the user to malicious links or email spam.

Social Engineering

This is a more direct way of hacking without using a system. Here the hacker gets the information by using some of the social engineering tactics. Here the hacker gets the trust of the user and makes them reveal their password or other information. The hackers play the role of the users who cannot access his account.

Trojan Horses

A Trojan horse is a malware program which is non self replicating. They can be used for gathering confidential formation like passwords. It acts like a backdoor for unauthorized access for the systems that are affected. They cannot be detected easily. These provide remote access to hackers. Trojan horse is a small program which pretends to do one thing but in reality it does another. These are used as gateways for the intruder to gain access. They stay on the victim's computer and send information to the intruder. The Trojan horse got its name from the old Greek mythology where they sent in a horse which didn't seem like a threat but resulted in the downfall of Troy.

Viruses

Virus is a program that self replicates. It spreads by adding copies of itself in the executable parts of code or documents. Many viruses are considered malicious but some of them are harmless. Viruses are of many types. Some of the viruses store passwords and other login data and send them to the hacker who created it. Once connected to the Internet these viruses contact the hacker with the gathered information.

Worm

Warm is an example of a hacking tool. Worms are basically used for detecting the weak spots in a given operating system. Hackers can use this information for hacking a particular computer system. These worms are downloaded to your computer system without your knowledge. A worm is also a self propagating program. Unlike virus, worm propagates using the network. It is harmless but it uses up the system resources. These send the information required by the hackers to them.

Chapter 3: Hacking Software and Hardware

Hacking software

There are many hacking software that you can make use of to make the job simpler. What these do is try out all the above mentioned approaches, one after the other, and try and crack the password. They will take a little time as they prefer to try the easier ones first and then move to the tougher techniques. But if you are really desperate and wish to crack a password at any cost, then it is best that you consider using hacking software.

Hacking Hardware

And you thought only softwares could do the job for you. Hacking hardware refers to a network of computers that will all work together to help find your password. These networks of computers can be rented for a fee and will work at lightning speed to find your password. They are better known as botnets and are meant to only serve the purpose of cracking passwords.

Similarly, GPUs are designed to help hack a password and are much more powerful than your regular CPUs. Graphical processing units will make use of a video card to find your password at a superfast speed.

Apart from these, there are also small devices that have been built to cater to hacking account passwords. They might look small but will work faster than a few hundred CPUs, all combined. These will make for great gizmos but you must be willing to shed 2000$ upwards, to buy a single unit.

Fighting viruses

Viruses can wreak havoc in your computer system and cause you to lose files, pictures, videos, have your passwords compromised etc. So it becomes all the more important for you to protect your system against these viruses and here are some ways in which you can do so.

- The very first step is for you to have an anti virus installed. The antivirus will work over time, if need be, but keep your systems clean and root out any virus. But make sure to update your program on a monthly basis as an old, and redundant, file will be of no use.
- Be careful of what you click on when you are online. It is obvious that your computer will not suffer from a virus attack just by being on a web page or

website. You will have to open or launch an infected file in order for it to attack your computer and so, be sure to click on safe links.

- Make sure you have a back up file for each of your important documents, and files, and spread it over several devices to help keep them safe.

Chapter 4: How to Hack an Email Password?

Hacking a password can sound both cool and illegal at the same time, but is it really as simple to crack one and access another person's personal account? Well, let's find out. Hacking a password, or cracking a password, refers to retrieving a secure password by running through data that is stored in a computer system or transported from it.

This can be done manually by entering the password, or allow the computer to run an algorithm that will try out several passwords until the right one is discovered. People hack passwords for several reasons such as to avail bank information or to look for an important email, but all with the same goal; to avail unauthorized access into someone's personal account.

This makes it highly illegal and can land the hacker in big trouble. But doing it the right way can help prevent the owner of the account from knowing that their password has been compromised, and the hacker can escape scot-free.

Over the past decade, hacking has become just so prominent that most email providers and social media platforms ask the account owner to use a strong password and include one capital letter, a number and also a symbol. This causes people to select a unique password that is not easy to crack. There is also the facility of sending email notifications if someone tries to enter the password several times or is trying to enter it from a different country. All this makes it very difficult to hack a password.

However, it is still possible to hack one, regardless of whether it is 8 letters long or 20 or has alpha- numeric values or not.

You can manually try and enter passwords that you think will work. For this, you must bear in mind a few principles that guide people's choice for passwords. To make it easy, you can go through a list that has been compiled containing the most common passwords that people use to secure their accounts, and you just might find yours there.

But manually doing it might take a lot of time and you can end up leaving behind uncovered tracks, which might get you in trouble. So instead, you can trust your computer to do all the hard work, while you sit back and relax.

For that, here are some techniques that can be employed to successfully hack a password.

Dictionary

The dictionary approach is one wherein the computer runs a set of dictionary words to check if any of them will match the correct password. This approach is not practical to be done manually, as it will take you forever to type in each word. A special software application can be used to run the words and it will take only a few seconds for the computer to find the right one. This technique is considered as the first approach since the results are almost always guaranteed. But if there is a unique password that's been used which contains a random mixture of alphabets, numerals and symbols then this technique will not work.

Hybrid

The hybrid is designed to tackle the problem of passwords that contain numbers and symbols. It will run several words along with numbers and symbols and also various permutations and combinations of the same. This will help you crack the password in no time, provided you are using the right set of dictionary words, numbers and symbols.

Rainbow table

Rainbow table is considered to be the next best approach, as modern systems use a different method to store passwords. What they do is add a hash before the password. So even if you were to find your way to the place that stores these passwords, you would still have to decrypt it. Instead of that, what you could do is add a hash before each of your dictionary words and compare it to the hashed password, if you are lucky, then you will find a perfect match.

Brute force

Brute force is considered the ultimate tool when it comes to cracking a password and is also the most CPU intensive method. The technique makes use of a large combination of alphabets, numbers and symbols and tries out all possible permutation and combination of each. So you can imagine the number of words that it will test and surmise the time that it will take to produce your word. This technique is considered the last resort by several hackers as it is quite time consuming.

Chapter 5: Few General Tips Of Computer Safety

The previous chapters have made you aware about the entire concept of hacking, the different tools of hacking, hacking emails and viruses. Now we will look at some information to secure your computer systems and networks from hacking attacks from other hackers. This will ensure that you are not just adept at the art of hacking, but you are also equipped to fight off other hackers.

Here are some important tips that go with the guidelines of computer safety:

- Avoid opening mails from unknown and untrusted sources. Never make the mistake of downloading attachments from such mails.

- It is advisable to visit only trusted websites on the net, as it is risky to visit an untrusted website which could pose a threat of malware infection. It is important to utilize the services of site advisor software like McAfee, which reports whether visiting a website is safe or not. Such software ensures safe browsing.

- Before installing new software or a program, it is advisable to completely uninstall all the files belonging to the old software or program.

- Make sure that you regularly update the software present on your system with the latest versions.

- It is advised that work-at-home professionals seek the help and services of network security experts to ensure that their system and network are well protected.

- Never respond to messages or chat requests from strangers, especially if you are suspicious of their authenticity.

- It is very important to create and maintain a backup of the files you need in an external memory or source. That way, even if you unexpectedly lose data from your system, you can still retrieve it from the external source.

- Some features of web browsers that are enabled by default, may introduce security issues into the system. Features like Java and ActiveX should be deactivated when not necessary.

- It is advisable to use a web browser which is known to offer essential security and safety features. For example, security experts advise using Mozilla Firefox for browsing the net, as it provides more security and safety features when compared to browsers like Internet Explorer.

- Computers running on operating systems like Linux or Macintosh are less vulnerable to hacking attacks when compared to the ones running on the hugely popular Windows. Try shifting to Linux or Macintosh, if you feel you can get accustomed to using them.

- Always remember that it is not possible to hack a computer that is switched off. So, remember to always shutdown your computer when not using it. Do not put it into sleep mode unnecessarily and limit the sleep mode time to twenty minutes at most

Conclusion

With this, we have now come to the end of this book. I have explained all the concepts of hacking in a very lucid and comprehensible fashion; however, putting them all into practice may sometimes be a bit tough. You can practice ethical aspects of hacking to improve your skills. Do not think twice before seeking help from professional security specialists if you feel all this is a bit too technical for you.

By now you must having a good idea about what hacking is and what will be the consequences if your system is attacked by an external or internal party. But fear not, simply follows the instructions and guidelines provided in this book and you can be rest assured that your system is well protected.

And please note that the world of computers is an ever changing and advancing one. The more advanced the system, the more you need to improve your knowledge. Always keep your software and system updated against other hackers and keep your system safe.

Thank you again for choosing this book and I hope you enjoyed the information shared.